Advisory Action Before the Filing of an Appeal Brief	**Application No.** 10/734,935	**Applicant(s)** SIMPSON ET AL.	
	Examiner Samson B. Lemma	**Art Unit** 2432	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 10 December 2008 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:
   a) ☐ The period for reply expires _____months from the mailing date of the final rejection.
   b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

   Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☐ They raise the issue of new matter (see NOTE below);
   (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☐ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☐ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: _____.
   Claim(s) objected to: _____.
   Claim(s) rejected: _____.
   Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.
12. ☐ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____
13. ☐ Other: _____.

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2434

Continuation of 11. does NOT place the application in condition for allowance because: Applicant's remark/arguments have been fully considered but they are not persuasive.

The claims are not amended and the argument is similar to argument presented previously. Thus Examiner assets that the previous final office action set forth previously is still applicable.

Examiner further would like to point out that, a careful reading reference/s on the record reveals that argument presented and features argued are indeed taught/disclosed by this reference/s on the record.

For clarification purpose, Examiner hereafter shows how the reference meets each and every limitation recited in independent claims argued by the applicant's representative.

Regarding independent claims 1 and 21 Carter discloses a method for controlling access to a document, [Abstract] comprising:

- Determining an access right for a user; (Column 12, lines 56-63; column 15, lines 62-67; abstract and column 8, lines 27-29) (Access Control Methods FIGS. 4-9 illustrate one method according to the present invention for controlling collaborative access to the work group document 90. In particular, the method includes computer-implemented steps for collaboratively encrypting the document 90 (FIG. 6) and steps for restricting access to the data portion 94 of the collaboratively encrypted document (FIG. 9)).
- building a member definition [Figure 5, see "member definition"] comprising a member identifier [Figure 5, ref. Num "98", See "member identifier"], an access control list [See column 12,lines 56-57; column 13, lines 52-62, see figure 5, ref. Num 100, "encrypted document key" signed by the public key of the member. Only the member with the corresponding private key can access the document. In particular see the following which is disclosed on column 13, lines 64-column 14, lines 5, "The encrypted document key 100 is formed by encrypting the document key obtained during the step 110 with the public key of the member in question, which was obtained during the step 116. Note that the underlying document key is the same for each member of the collaborative group, but the encrypted form 100 of the document key is unique to each member. Those of skill in the art will appreciate. that the encrypted document key 100 can be decrypted only by using the private key 80 that corresponds to the public key 78 used to encrypt the document-key. "See also "collaborative access controller 44" which is described on column 6, lines 11-22 as the access controller which restrict access to the members only. Non members are restricted form accessing the information. See for instance the following disclosed on column 6, lines 11-12, "users who are currently members of a collaborative group can readily access the information, while users who are not currently members of the group cannot"] and a digital signature,[See also figure 5, ref. Num "102", "encrypted message digest", signed by the private key. In particular see what is disclosed on column 14, lines 15-21, "the encrypted message digest 102 is formed by generating a message digest based on the current contents of the data portion 94 of the document 90 and then encrypting that message digest with the private key 80 of the member who is signing the document 90." See also the abstract and column 6, lines 11-12, "collaborative signatures, such that members of the group can digitally sign a particular version of the data portion. These collaborative signatures can then be used to advantage in ways similar to conventional individual digital signatures. For instance, the collaborative signatures can be used to identify the signing member."] and associating the member definition with the user. [Figure 5 and column 6, lines 11-22, See "Users who are currently members of a collaborative group can readily access the information, while users who are not currently members of the group cannot"]

and

- Linking the member definition to a portion of a document. [Figure 6, ref. Num "120"] ("Link member definition(s) with document.")

Carter does not explicitly disclose

linking the member definition to a first data portion of a document, wherein the document has the first data portion and a second data portion,

receiving a request from the user to access the document; comparing the request with the access right; and allowing access to only the first data portion in accordance with the access right

However, in the same field of endeavor, Rider discloses,

Linking the member definition to a first data portion of a document, wherein the document has the first data portion and a second data portion, [paragraph 0044, figure 4A & 0034-0035] (As shown, document 400 includes descriptor portion 402 and data portion 404. Descriptor portion 402 can include basic information about the device and its operation whereas data portion 404 can include actual data, which can be employed by specific applications. Portion 406 is a portion of data 404 that has its access governed in accordance with the principles of tier two security as described herein. That is, one or more access rights can be associated with portion 406. Although one portion 406 is shown, an ordinarily skilled artisan will appreciate that the same or other access rights can govern other portions of data portion 404.)

Receiving a request from the user to access the document; comparing the request with the access right; and allowing access to only the first data portion in accordance with the access right [Paragraph 0034-0035 paragraph 0044, figure 4A] (On paragraph 0034, the following has been disclose. Moreover, security manager 170 can permit, restrict or completely deny a user request to access one or more documents as well as the contents of those documents. A document or a portion thereof can represent a command for, or a configuration of, one of devices 135 such as a router or switch. Security manager 170 governs by determining whether a particular user has access rights to a specific network resource, a particular document or only a portion of a document. Furthermore on paragraph 0035, the following has been disclosed. "By restricting access in relation to a document's content, a more fine-grained approach to configuring, managing and monitoring network resources is realized. Hence, tier two security restricts a user to data constituting a portion of an entire document rather than providing complete or no access to that document. For example, FIG. 4A depicts document portion 406 that is accessible. Note that other portions of document 400 are not necessarily accessible to that user.")

Regarding independent claim 11 Carter discloses a method for controlling access to a document, [Abstract] comprising:

- A document comprising a first data and a second data.["the documents, which are indicated as 4, ref. Num "92" could be

more than one as it is indicated on column 14, lines 23-24 and figure 4-6, the system builds one or more member definitions which is associated with one or more documents.]
a first member definition [figure 5, ref. Num "96", "Member definition "] associated with the first data[See figure 4, ref. Num "92"/"document "] wherein the first member definition contains a first user identifier [Figure 5, ref. Num "98"] and a first access right for a first user for the first data [Figure 5, ref. Num "100"; see the "encrypted document key" which is encrypted by the member's public key. Only the Member who has access to the information could use his corresponding private key to decrypt and get the document key which allows the member to access the document. In particular see the following which is disclosed on column 13, lines 64-column 14, lines 5, "The encrypted document key 100 is formed by encrypting the document key obtained during the step 110 with the public key of the member in question, which was obtained during the step 116. Note that the underlying document key is the same for each member of the collaborative group, but the encrypted form 100 of the document key is unique to each member. Those of skill in the art will appreciate. that the encrypted document key 100 can be decrypted only by using the private key 80 that corresponds to the public key 78 used to encrypt the document-key."] ;
As it is indicated 14, lines 23-24 and figure 4-6, the system builds one or more member definitions. And the member definitions shown on figure 5, is associated to the documents shown on figure 4. Even though only one document is shown on figure 4, ref. Num "54, 90" the system is built for one or more documents. See the documents described on column 9, lines 35.
Thus the following is also correct.
a second member definition [figure 5, ref. Num "96", "Member definition "] associated with the second data [See figure 4, ref. Num "92"/"document "], wherein the second member definition contains a second user identifier[Figure 5, ref. Num "98"] and a second access right for a second user for the second data; [Figure 5, ref. Num "100"; see the "encrypted document key" which is encrypted by the member's public key. Only the Member who has access to the information could use his corresponding private key to decrypt and get the document key which allows the member to access the document. In particular see the following which is disclosed on column 13, lines 64-column 14, lines 5, "The encrypted document key 100 is formed by encrypting the document key obtained during the step 110 with the public key of the member in question, which was obtained during the step 116. Note that the underlying document key is the same for each member of the collaborative group, but the encrypted form 100 of the document key is unique to each member. Those of skill in the art will appreciate. that the encrypted document key 100 can be decrypted only by using the private key 80 that corresponds to the public key 78 used to encrypt the document-key."] ;
Carter does not explicitly disclose
Wherein the document has the first data portion and a second data portion,
receiving a request from the user to access the document; comparing the request with the access right; and allowing access to only the first data portion in accordance with the access right
However, in the same field of endeavor, Rider discloses,
Linking the member definition to a first data portion of a document, wherein the document has the first data portion and a second data portion, [paragraph 0044, figure 4A & 0034-0035] (As shown, document 400 includes descriptor portion 402 and data portion 404. Descriptor portion 402 can include basic information about the device and its operation whereas data portion 404 can include actual data, which can be employed by specific applications. Portion 406 is a portion of data 404 that has its access governed in accordance with the principles of tier two security as described herein. That is, one or more access rights can be associated with portion 406. Although one portion 406 is shown, an ordinarily skilled artisan will appreciate that the same or other access rights can govern other portions of data portion 404.)
Receiving a request from the user to access the document; comparing the request with the access right; and allowing access to only the first data portion in accordance with the access right [Paragraph 0034-0035 paragraph 0044, figure 4A] (On paragraph 0034, the following has been disclose. Moreover, security manager 170 can permit, restrict or completely deny a user request to access one or more documents as well as the contents of those documents. A document or a portion thereof can represent a command for, or a configuration of, one of devices 135 such as a router or switch. Security manager 170 governs by determining whether a particular user has access rights to a specific network resource, a particular document or only a portion of a document. Furthermore on paragraph 0035, the following has been disclosed. "By restricting access in relation to a document's content, a more fine-grained approach to configuring, managing and monitoring network resources is realized. Hence, tier two security restricts a user to data constituting a portion of an entire document rather than providing complete or no access to that document. For example, FIG. 4A depicts document portion 406 that is accessible. Note that other portions of document 400 are not necessarily accessible to that user.")

In view of this understanding, each and every limitation recited in the claims is disclosed by the reference on the record and the rejection is maintained.

Examiner encourages applicant's representative to schedule a telephone interview so that the claim limitations with respect to the art on the record are further discussed.

..